UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF MISSISSIPPI
NORTHERN DIVISION

EBONY HEMPHILL, individually and on behalf of all others similarly situated — PLAINTIFF

V. — CIVIL ACTION NO. 3:24-CV-74-KHJ-ASH

HORNE, LLP — DEFENDANT

consolidated with

TERRY CHIZEK, on behalf of himself individually and on behalf of all others similarly situated — PLAINTIFF

V. — CIVIL ACTION NO. 3:24-CV-178-KHJ-ASH

HORNE, LLP — DEFENDANT

ORDER

Before the Court is Defendant Horne, LLP's [17] Motion to Dismiss Plaintiffs Ebony Hemphill and Terry Chizek's [28] Second Amended Consolidated Class Action Complaint (Second Amended Complaint). *See also* Joint Notice on Corrected Compl. [27] at 1.[1] For the reasons stated below, the Court grants Horne's [17] Motion to Dismiss and dismisses Hemphill and Chizek's claims without prejudice for lack of standing.

[1] Hemphill filed a class action against Horne in February 2024, and Chizek followed suit the next month. *See* Compl. [1]; Complaint, *Chizek v. Horne, LLP*, No. 3:24-CV-178 (S.D. Miss. filed Mar. 27, 2024). In April, the Court consolidated the two class actions, so Hemphill and Chizek filed a [16] Consolidated Class Action Complaint. *See* Order [15]. They have since clerically amended their consolidated complaint twice, and Horne consented to the filing of the now-operative [28] Second Amended Complaint. [27] at 1 (noting that parties agree new complaint does not moot [17] Motion to Dismiss).

I. Background

This putative class action involves a data breach of Horne's computer network in 2021, which permitted a hacker to access certain systems containing Hemphill and Chizek's personally identifiable information (PII). [28] ¶¶ 2–3; Horne Notice Letter [28-1] at 2. Horne is an accounting firm that serves many business clients, including University of Mississippi Medical Center (UMMC) and Memorial Hospital Gulfport (Memorial). [28] ¶¶ 24–25, 30–31, 33. Hemphill and Chizek received medical services from UMMC and Memorial, respectively. *Id.* ¶¶ 24–25. As a result, Hemphill and Chizek supplied certain PII—including their Social Security numbers—to their medical providers who, in turn, gave it to Horne. *See id.* ¶¶ 40, 118, 133.[2] From December 8, 2021, to December 13, 2021, a hacker gained access to certain systems in Horne's network and managed to extract an unknown amount of PII from the network. *Id.* ¶¶ 42–43.

In early 2024, Hemphill and Chizek received letters from Horne notifying them of the 2021 data breach. *Id.* ¶¶ 119, 134. The letters informed Hemphill and Chizek that "certain information relating to [them] may have been within the accessed systems, including [their] name[s] and health insurance information and patient account number[s]." [28-1] at 2; *see also* [28] ¶¶ 119, 134 (indicating that Hemphill and Chizek received identical letters). But the letters also noted that Horne "was unable to confirm what information within those systems was actually

[2] Hemphill also formerly worked for Horne and provided Horne with PII during her employment. *See* [28] ¶ 118.

accessed" and had no "evidence to indicate that [Hemphill or Chizek's] information was subject to actual or attempted misuse" because of the breach. [28-1] at 2.

In the summer of 2023, someone tried to access Hemphill's bank account, and she had to personally visit the bank to resolve the matter. [28] ¶ 121. After receiving the [28-1] Notice Letter, Hemphill also froze her credit, changed her email passwords, started monitoring her accounts, and consulted with a law firm. *Id.* ¶¶ 123–24. As for Chizek, at an unspecified time after the breach, an unknown party placed credit-card inquiries on his credit report, which damaged his credit score. *Id.* ¶ 136. TransUnion also informed him at some point that his private information had been disseminated on the dark web,[3] and he later experienced an increase in spam calls, texts, and emails. *See id.* ¶¶ 137–38.

From these facts, Hemphill and Chizek allege that their "highly sensitive personal information . . . was compromised and unlawfully accessed and extracted during the [d]ata [b]reach." *Id.* ¶ 10. For her part, Hemphill states that she "already experienced identity theft" because someone tried to access her account. *Id.* ¶ 121. And Chizek alleges solely "upon information and belief" that the data breach caused each of the later negative events he experienced. *Id.* ¶¶ 136–38. Ultimately, Hemphill and Chizek both allege they suffered the same six injuries from the breach: (1) exposure, theft, and misuse of their PII, *id.* ¶¶ 10, 49, 119, 134; (2)

[3] "The dark web is an area of the internet accessible only by using an encryption tool. It provides anonymity and privacy online, and perhaps consequently, frequently attracts those with criminal intentions." *United States v. Schultz*, 88 F.4th 1141, 1142 n.1 (5th Cir. 2023) (citing Gareth Owen & Nick Savage, Glob. Comm'n on Internet Governance, *The Tor Dark Net* 1 (2015)).

exposure to substantial and imminent risk of identity theft, *id.* ¶¶ 107, 130, 145; (3) lost time and increased anxiety from undertaking mitigation efforts, *id.* ¶¶ 128, 143; (4) lost privacy, *id.* ¶ 101; (5) lost benefit of a bargain with Horne, *id.* ¶ 100; and (6) diminished value of their PII, *id.* ¶¶ 127, 142. *See also* Resp. Opp'n Mot. Dismiss [22] at 9–15.

Horne now moves to dismiss the [28] Second Amended Complaint for lack of subject-matter jurisdiction and failure to state a claim. Mem. Supp. Mot. Dismiss [18] at 1–2. It first argues that Hemphill and Chizek lack standing to sue because they have not established the first two elements of standing: an injury in fact and a causal connection between an injury and Horne's conduct. *Id.* In the alternative, Horne contends that Hemphill and Chizek have failed to establish Horne's duty to protect them from the hacker's criminal actions. *Id.* at 2.

II. Standard

A. Rule 12(b)(1)

Parties may challenge a district court's subject-matter jurisdiction over a case by filing a motion under Federal Rule of Civil Procedure 12(b)(1). A federal court's subject-matter jurisdiction only extends to "Cases" and "Controversies." *Murthy v. Missouri*, 603 U.S. 43, 56 (2024) (quoting U.S. Const. art. III, § 2, cl. 1). A "case or controversy exists only when at least one plaintiff establishes . . . standing to sue." *Id.* at 57 (cleaned up). Since Article III standing is a jurisdictional issue, courts consider challenges to a plaintiff's standing under Rule 12(b)(1). *See Crane v. Johnson*, 783 F.3d 244, 250–51 (5th Cir. 2015). The plaintiff always bears the

burden of establishing standing. *NAACP v. Tindell*, 95 F.4th 212, 216 (5th Cir. 2024) (per curiam).

A Rule 12(b)(1) motion may either facially challenge the complaint's jurisdictional allegations or present evidence challenging the jurisdictional facts underlying the complaint. *Superior MRI Servs., Inc. v. All. Healthcare Servs., Inc.*, 778 F.3d 502, 504 (5th Cir. 2015); *see also Cell Sci. Sys. Corp. v. La. Health Serv.*, 804 F. App'x 260, 262–64 (5th Cir. 2020) (per curiam) (explaining facial and factual Rule 12(b)(1) motions). Thus, a court may find that it lacks subject-matter jurisdiction based on "(1) the complaint alone; (2) the complaint supplemented by undisputed facts evidenced in the record; or (3) the complaint supplemented by undisputed facts plus the court's resolution of disputed facts." *Cantu Silva v. United States*, 110 F.4th 782, 786 (5th Cir. 2024) (cleaned up).

When considering a facial challenge, courts examine "the sufficiency of the [well-pleaded, factual] allegations in the complaint because they are presumed to be true." *Lee v. Verizon Commc'ns, Inc.*, 837 F.3d 523, 533 (5th Cir. 2016) (cleaned up); *see also Daniel v. Univ. of Tex. Sw. Med. Ctr.*, 960 F.3d 253, 256 (5th Cir. 2020). In such cases, a "district court should dismiss where it appears certain that the plaintiff cannot prove a plausible set of facts that establish subject-matter jurisdiction." *Bank of La. v. FDIC*, 919 F.3d 916, 922 (5th Cir. 2019) (cleaned up); *see also Tyler v. Hennepin County*, 598 U.S. 631, 637 (2023). But when there is a factual challenge, courts resolve disputed facts without presuming that the complaint's allegations are true. *See Cantu Silva*, 110 F.4th at 786. To survive a

factual attack, a plaintiff must present counterevidence that proves subject-matter jurisdiction by a preponderance of the evidence. *Superior MRI Servs.*, 778 F.3d at 504.

If a party files a Rule 12(b)(1) motion alongside other Rule 12 motions, courts first consider the jurisdictional attack before reaching any merits-based challenges. *Porretto v. City of Galveston Park Bd. of Trs.*, 113 F.4th 469, 481 (5th Cir. 2024). A court without subject-matter jurisdiction may not reach the merits and must dismiss the case without prejudice under Rule 12(b)(1). *Spivey v. Chitimacha Tribe*, 79 F.4th 444, 448–49 (5th Cir. 2023).

B. Rule 12(b)(6)

Federal Rule of Civil Procedure 12(b)(6) permits the dismissal of a complaint if it fails "to state a claim upon which relief can be granted." When reviewing a complaint under Rule 12(b)(6), the Court only considers the complaint, documents attached to or incorporated in it, and matters subject to judicial notice. *Benfer v. City of Baytown*, 120 F.4th 1272, 1278 n.2 (5th Cir. 2024). The Court must accept all factual allegations in the complaint as true, but it is not bound to accept legal conclusions, conclusory statements, or bare assertions without factual support. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). And if a complaint's exhibits contradict its allegations, the exhibits control. *Stevenson v. Tocé*, 113 F.4th 494, 502–03 (5th Cir. 2024). To survive a motion to dismiss, a complaint must include enough factual allegations to state a facially plausible claim to relief. *Iqbal*, 556 U.S. at 678. A

claim has facial plausibility if the Court may reasonably infer the defendant's culpability from the facts the plaintiff alleges. *Id.*

If a complaint fails to satisfy Rule 12(b)(6), courts should liberally grant leave to amend "when the plaintiff might be able to state a claim based on the underlying facts and circumstances." *Ass'n of Am. Physicians & Surgeons Educ. Found. v. Am. Bd. of Internal Med.*, 103 F.4th 383, 394 (5th Cir. 2024) (cleaned up). But if amendment would be futile, a Rule 12(b)(6) dismissal should be with prejudice. *See HCB Fin. Corp. v. McPherson*, 8 F.4th 335, 345–46 (5th Cir. 2021); *see also Jacquez v. Procunier*, 801 F.2d 789, 792 (5th Cir. 1986) ("At some point a court must decide that a plaintiff has had fair opportunity to make his case; if, after that time, a cause of action has not been established, the court should finally dismiss the suit.").

III. Analysis

The Court lacks subject-matter jurisdiction over Hemphill and Chizek's claims because they lack standing to sue for damages or injunctive relief. Since Horne does not support its [17] Motion to Dismiss with evidence, it mounts a facial attack, and the Court considers only the [28] Second Amended Complaint's allegations. Those allegations do not establish standing for Hemphill and Chizek's damages' claims: Hemphill has not suffered an injury in fact, and though Chizek has, he fails to establish a causal connection between any injury and the data breach. Both also lack standing to bring their injunctive claims because they have not shown an immediate threat of another data breach. As this lack of standing deprives the Court of subject-matter jurisdiction, the Court grants Horne's [17]

Motion to Dismiss without proceeding to the merits of Hemphill and Chizek's claims. *See Spivey*, 79 F.4th at 448–49.

A. Damages Claims

Standing to sue for damages exists when (1) a plaintiff "has suffered or likely will suffer an injury in fact"; (2) the "injury likely was caused or will be caused by the defendant"; and (3) the "injury likely would be redressed by the requested judicial relief." *FDA v. All. for Hippocratic Med.*, 602 U.S. 367, 380 (2024). At the pleading stage, a plaintiff must "clearly allege facts demonstrating each element" of standing. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (cleaned up). And plaintiffs "must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 431 (2021). As Horne only contests the first two elements of standing for each claim, the Court focuses on those. *See* [18] at 5–14.

1. Injury in Fact

An injury in fact must be "concrete, particularized, and actual or imminent . . . ." *Murthy*, 603 U.S. at 57 (cleaned up). First, concreteness requires that the injury "be real and not abstract." *All. for Hippocratic Med.*, 602 U.S. at 381. Naturally, tangible harms—such as physical or monetary harms—are concrete. *TransUnion*, 594 U.S. at 425. But intangible harms can also be concrete if they have "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." *Id.* Second, particularization requires the injury to

"affect the plaintiff in a personal and individual way . . . ." *All. for Hippocratic Med.*, 602 U.S. at 381 (cleaned up).

Third, actuality or imminence requires that the injury (1) have already occurred, (2) be certainly impending, or (3) be at substantial risk of occurring. *See Dep't of Com. v. New York*, 588 U.S. 752, 767 (2019). Thus, "allegations of *possible* future injury" or theories of injury that rest "on a highly attenuated chain of possibilities" are not sufficient. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409–10 (2013) (cleaned up). And specific to damages actions, "the mere risk of future harm, standing alone, cannot qualify as a concrete harm" unless "the exposure to the risk of future harm itself causes a *separate* concrete harm." *TransUnion*, 594 U.S. at 436.

a. Exposure, Theft, and Misuse of PII and Loss of Privacy

The Fifth Circuit has only briefly considered standing in the context of a data breach case. *See Ellis v. Cargill Meat Sols.*, No. 24-10339, 2024 WL 4692024, at *3 (5th Cir. Nov. 6, 2024) (per curiam). But other circuits have had more occasions to apply *Clapper*, *Spokeo*, and *TransUnion* in such cases. *See Williams v. Bienville Orthopaedic Specialists, LLC*, 737 F. Supp. 3d 411, 417–20 (S.D. Miss. 2024) (surveying Supreme Court and out-of-circuit precedent on standing in data-breach cases). The Court starts with the only principle that courts uniformly agree on: The misuse of PII—that is, identity theft—constitutes an actual, concrete injury. *See, e.g.*, *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 373 (1st Cir. 2023); *see*

also Merrell v. 1st Lake Props., Inc., No. 2:23-CV-1450, 2023 WL 6316257, at *3 (E.D. La. Sept. 28, 2023) (collecting cases).

From there, courts begin to diverge. Going one step further, the Second Circuit has held that mere exposure of private PII to unauthorized actors, even without misuse or risk of misuse, constitutes a concrete injury. *Bohnak v. Marsh & McLennan Cos.*, 79 F.4th 276, 285–86 (2d Cir. 2023). Relying on *TransUnion*, the court in *Bohnak* noted "that 'disclosure of private information' was an intangible harm 'traditionally recognized as providing a basis for lawsuits in American courts.'" *Id.* at 286 (quoting *TransUnion*, 594 U.S. at 425). And since the exposure of private PII bears a close relationship with the disclosure of private information, the court determined that the exposure of private PII constitutes a concrete injury. *Id.* at 285–86. To the contrary, the Eleventh and Fourth Circuits still typically require the misuse of any PII before recognizing that an injury in fact has occurred. *See Green-Cooper v. Brinker Int'l, Inc.*, 73 F.4th 883, 889 (11th Cir. 2023) (cleaned up), *cert. denied sub nom. Brinker Int'l, Inc. v. Steinmetz*, 144 S. Ct. 1457 (2024) (mem.); *O'Leary v. TrustedID, Inc.*, 60 F.4th 240, 244 (4th Cir. 2023).

So does a concrete injury occur when thieves access and steal private PII in a data breach or only after the thieves use that data to steal someone's identity? This question orients the injury-in-fact analysis, but the Court need not choose a side today. Hemphill fails to plausibly allege that any of her private PII has been exposed, much less misused, and Chizek plausibly alleges that his private PII was both exposed and misused.

Even under the Second Circuit's more forgiving approach, only the exposure of "private PII"—like a Social Security number—inflicts an injury in fact. *Bohnak*, 79 F.4th at 285; *see also Farst v. AutoZone, Inc.*, 700 F. Supp. 3d 222, 231–32 (M.D. Pa. 2023). This is because the tortious disclosure of private information traditionally requires publication of (1) "private facts" that (2) "would be highly offensive to a reasonable person" and (3) are "not of legitimate concern to the public." *Taylor-Travis v. Jackson State Univ.*, 984 F.3d 1107, 1116 (5th Cir. 2021) (citing Restatement (Second) of Torts § 652D (Am. L. Inst. 1977)). Since PII is a broad term, it encompasses any identifying information. *See, e.g.*, [28] ¶ 40. But not all identifying information is private such that its exposure would inflict a "traditionally recognized" harm. *TransUnion*, 594 U.S. at 425; *Johnson v. Sawyer*, 47 F.3d 716, 734 (5th Cir. 1995) (en banc) (noting that someone's "name or other identifying public facts" like the person's "middle initial, age, [or] street address" typically constitute "nonprivate information"). To allege a concrete injury, Hemphill and Chizek must plausibly plead that their *private* PII was exposed.

With that in mind, the Court turns to the [28] Second Amended Complaint's allegations. In various places, Hemphill and Chizek assert that their private PII, including financial information and Social Security numbers, "was accessed and stolen in the [d]ata [b]reach." *E.g.*, [28] ¶ 49; *see also id.* ¶¶ 17, 40, 44, 47, 102–03, 118–19, 133–34. But the well-pleaded facts in the [28] Second Amended Complaint reveal that Hemphill and Chizek are only speculating about whether their PII was stolen. *See, e.g.*, *id.* ¶¶ 5, 129, 144; [28-1] at 2; *see also* [28] at 1 ("Plaintiffs make

the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.").

Hemphill and Chizek's reliance on modal verbs of possibility to plead their allegations underscores this fact. *Cf. Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011) ("[O]ne cannot describe how the plaintiffs will be injured without beginning the explanation with the word 'if.'" (cleaned up)). They allege only that a hacker "*may have* . . . exfiltrated certain files containing" their PII. [28] ¶ 5 (emphasis added). They "*believe*[]" their PII "*may have* already been sold by the cybercriminals." *Id.* ¶¶ 129, 144 (emphasis added). They fear cybercriminals "*may exploit*" their PII by selling it on the dark web. *Id.* ¶ 102 (emphasis added). And they "*may* also *incur* out of pocket costs for . . . protective measures to . . . detect identity theft." *Id.* ¶ 20 (emphasis added).

Moreover, the [28-1] Notice Letter attached to the [28] Second Amended Complaint confirms that "certain information relating to [Hemphill and Chizek] *may have been* within the accessed systems, including [their] name[s] and health insurance information and patient account number[s]." [28-1] at 2 (emphasis added); *see also Stevenson*, 113 F.4th at 502–03. The [28-1] Notice Letter also shows that Hemphill and Chizek's conclusory allegations about the exposure of their financial information and Social Security numbers are doubly speculative. *See* [28] ¶¶ 17, 40, 44, 47, 102–03, 118, 133. To support those allegations, they reference a notice of the breach sent to the Maine Attorney General's Office. *Id.* ¶ 44 & n.11; *see also Benfer*, 120 F.4th at 1278 n.2. That notice states that "the potentially impacted

data includes name, Social Security number, and financial account information."[4] From this, Hemphill and Chizek conclude that their financial information and Social Security numbers were exposed, too. *See, e.g.*, [28] ¶ 47.

But the notice also says that the potentially compromised information "varies for each individual." Notice of Data Event, *supra* note 4, at 2. And the [28-1] Notice Letter sent to Hemphill and Chizek informed them that their names, health insurance information, and patient account numbers were potentially exposed. [28-1] at 2. So they first speculate that the PII listed in the [28-1] Notice Letter was exposed before then hypothesizing that PII not listed in the letter was also exposed because the letter "did not expand on whether additional information was stolen as well." [28] ¶¶ 119, 134. Ultimately, these "naked assertions devoid of further factual enhancement" do not merit a presumption of truth. *Iqbal*, 556 U.S. at 678 (cleaned up).

Left with only the well-pleaded facts, the Court cannot reasonably infer that Hemphill's private PII was stolen. *See id.* As to Hemphill, only one fact supports an inference that someone stole her private PII: the unsuccessful attempt to access her bank account roughly 18 months after the breach. [28] ¶ 121. But Hemphill alleges no factual details about the fraud attempt. *See id.* To infer the exposure of Hemphill's private PII from the access attempt alone, the Court must conclude that

[4] Notice of Data Event from Horne, LLP to the Off. of the Me. Att'y Gen., at 2 (Dec. 26, 2023), https://www.maine.gov/ag/consumer/identity_theft/index.shtml [https://perma.cc/85K2-6TWL] (click "Maine Data Breach Notices"; then search for "Horne LLP" and follow hyperlink; then click on hyperlinked PDF of Notice).

the attempt required the use of her private PII. This inference would be highly speculative. Hemphill's allegations about the attempt say nothing about how it was accomplished. In fact, the failure of the attempt implies that the would-be fraudster lacked the private PII necessary to make the attempt successful. The sole fact of the attempt cannot support a reasonable inference that Hemphill's private PII must have been exposed.

On the other hand, Chizek's allegations can support a reasonable inference that his private PII was somehow exposed. He pleads several pertinent facts: (1) the credit-card inquiries placed on his credit report; (2) the alert from TransUnion that his private information was disseminated on the dark web; and (3) the increase of spam communications. *Id.* ¶¶ 136–38. Like Hemphill, Chizek alleges nothing more about these occurrences than that they happened. *See id.* And from the start, the Court notes that an increase in spam communications implies nothing about the exposure of private PII; such communications can be accomplished with nonprivate information like an email address or phone number.

Still, it is plausible that the placement of inquiries on Chizek's credit report required using his private PII. A Social Security number is generally required to open a credit card. Since someone placed credit-card inquiries on Chizek's credit report, the Court can infer that someone obtained access to Chizek's private PII and tried to open a credit card in his name. Likewise, Chizek alleges TransUnion told him that his "[p]rivate [i]nformation" was "disseminated on the dark web . . . ." *Id.* ¶ 137. At this stage, the Court "presume[s] that general allegations embrace those

specific facts that are necessary to support the claim." *Gen. Land Off. v. Biden*, 71 F.4th 264, 272 (5th Cir. 2023) (cleaned up). So the Court accepts Chizek's allegation that his private information was disseminated, even though he does not specify what that information is. This allegation plausibly pleads that Chizek's private PII was exposed and misused in some way. *See Green-Cooper*, 73 F.4th at 889.

b. Increased Risk of Identity Theft and Mitigation Costs

Chizek alone has also plausibly pleaded a concrete injury stemming from the substantial or impending risk of identity theft. When suing for damages based on the risk of future harm, plaintiffs must allege the risk itself inflicted separate concrete injuries. *TransUnion*, 594 U.S. at 436; *see also id.* at 437 ("[P]laintiffs did not . . . present evidence that . . . they suffered some other injury (such as an emotional injury) from the mere risk . . . ."); *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155–56 (3d Cir. 2022). Hemphill and Chizek have pleaded lost time, anxiety, and other costs associated with mitigating a substantial risk of identity theft as the separate concrete harms necessary for standing. [28] ¶¶ 128, 143. But plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending" or at substantial risk of occurring. *Clapper*, 568 U.S. at 416. So the real question is whether the risk of identity theft here is either substantial or certainly impending.

For Hemphill, it isn't. Simply put, her risk of identity theft is "too speculative to support standing." *Ellis*, 2024 WL 4692024, at *3. She makes "no [factual] allegation that any hacker, identity thief, or third party accessed [her] data." *Id.*

That a hacker "may have . . . exfiltrated certain files," [28] ¶ 5, that "may have been within the accessed systems" cannot create a substantial or certainly impending risk of identity theft. [28-1] at 2. And the unsuccessful attempt to access Hemphill's bank account does not make it plausible that someone possesses the PII necessary to place her at substantial risk of identity theft. Thus, her mitigation costs are not a concrete injury. *See Clapper*, 568 U.S. at 416.

In contrast, Chizek has alleged that someone possesses enough of his PII to attempt opening credit cards in his name. This is sufficient to plausibly plead a substantial risk of identity theft. Thus, his anxiety and mitigation costs are separate concrete harms. *See Clemens*, 48 F.4th at 157–58.

c. Lost Benefit of the Bargain

Hemphill and Chizek have not plausibly pleaded a concrete harm based on the lost benefit of a bargain with Horne. As to their benefit-of-the-bargain theory, Hemphill and Chizek claim that they "provided their PII to [Horne] or its third-party agents in exchange for Horne's services or employment. In exchange for the PII, [Horne] promised to protect their PII from unauthorized disclosure." [28] ¶ 192. Hemphill also alleges she provided certain PII during her employment with Horne. *See id.* ¶ 118. But she fails to plead what information she gave Horne as an employee or if any of that information was accessed. *See id.* She also pleads no facts about her employment agreement with Horne permitting the Court to infer that Horne had a contractual duty to protect her data as an employee. *See Clemens*, 48 F.4th at 156.

Outside of Hemphill's employment with Horne, both Hemphill and Chizek provided their PII only to Horne's clients—not Horne—in exchange for medical services (not Horne's services). *See* [28] ¶¶ 24–25. While they claim to have "entered into implied contracts with" Horne, *id.* ¶ 196, even an implied contract must arise "from a mutual agreement and intent to promise . . . ." *L & F Homes & Dev., L.L.C. v. City of Gulfport*, 538 F. App'x 395, 404 (5th Cir. 2013) (per curiam) (cleaned up). As patients, Hemphill and Chizek had no direct relationship with and received no services from Horne. *See, e.g.*, *Bednyak v. Fin. Risk Mitigation, Inc.*, No. 2:24-CV-25, 2024 WL 4869157, at *9 (E.D. La. May 31, 2024). Thus, the Court cannot infer that they had any mutual agreement with Horne or that Horne intended to promise them anything. They were strangers to Horne. For this reason, they fail to plausibly plead an injury stemming from the breach of an implied contract.

Even if Hemphill and Chizek had some sort of consumer relationship with Horne, they do not "allege facts showing how the price they paid for" medical services "incorporated some particular sum that was understood by both parties to be allocated towards the protection of customer data" by Horne. *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015); *see also Williams*, 737 F. Supp. 3d at 422. And most importantly, assuming that they had somehow bargained for data protection with Horne, Hemphill and Chizek still do not plead that their PII was stolen in the breach, only that it may have been stolen. *E.g.*, [28] ¶ 5. As a result, Hemphill and Chizek fail to allege that any potential implied contract was even breached.

d. Diminished Value of PII

Hemphill and Chizek also fail to plead a concrete injury based on the diminished value of their PII because of the breach. Some courts have "recognized that diminished value of PII can support Article III standing in a breach of contract case or where the plaintiff alleges actual misuse of" PII. *Bednyak*, 2024 WL 4869157, at *9 (citations omitted) (collecting cases). But Hemphill and Chizek "had no contract with" Horne "nor any privity whatsoever with the company," and they do "not allege actual misuse of [their] PII as a result of the" data breach. *Id.* Likewise, they have not "been denied credit on favorable terms, nor had problems verifying [their] identit[ies] and financial history . . . ." *Id.* Hemphill and Chizek's speculation that their PII's value has diminished because it might have been stolen in the breach "is not sufficiently concrete to satisfy the injury in fact requirement." *Id.*

2. Causation

After alleging an injury in fact, "a plaintiff must establish that there is a causal connection between the injury and the conduct complained of—the injury must be fairly traceable to the challenged action of the defendant . . . ." *Reule v. Jackson*, 114 F.4th 360, 367 (5th Cir. 2024) (cleaned up). So "plaintiffs attempting to show causation generally cannot rely on speculation about the unfettered choices made by independent actors not before the courts." *All. for Hippocratic Med.*, 602 U.S. at 383 (cleaned up). In that event, "the plaintiff must show that the third parties will likely react in predictable ways that in turn will likely injure the

plaintiffs." *Id.* (cleaned up). And "the links in the chain of causation . . . must not be too speculative or too attenuated." *Id.* (cleaned up).

Of Hemphill and Chizek, only Chizek has plausibly pled injuries in fact based on the exposure of his private PII. All the same, the traceability requirement dooms his claims. That his private PII was exposed says nothing about whether it was exposed *in the breach*. The Court has already noted the speculative nature of Chizek's allegations. *See supra* pp. 9–13. Since he does not allege that anyone accessed his private PII in the breach, the Court must try to reasonably infer that fact from the others alleged. It cannot.

As previously noted, Chizek alleges that (1) credit-card inquiries were placed on his credit report; (2) TransUnion alerted him that his private information was disseminated on the dark web; and (3) he has received increased spam communications. [28] ¶¶ 137–38. Chizek states that he "is very careful about sharing PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source." *Id.* ¶ 140. And he has pleaded "upon information and belief" that the inquiries, dissemination, and spam communications stem from the breach. *Id.* ¶¶ 136–38. But he does not allege that the inquiries were placed on his credit report using PII obtainable from the breach. *See id.* He also fails to plead that the PII disseminated on the dark web was the same PII involved in the breach. *See id.* And he never explains how someone could use his health insurance information or patient account number to place inquiries on his credit report. *See id.*

Chizek waves away these deficiencies by arguing that any challenge to traceability is procedurally premature at this stage because he lacks the benefit of discovery. [22] at 16–17. This argument relies on the premise that discovery will reveal what data was stolen in the breach. To be sure, the "*Twombly* plausibility standard . . . does not prevent a plaintiff from pleading facts alleged upon information and belief where the facts are peculiarly within the possession and control of the defendant or where the belief is based on factual information that makes the inference of culpability plausible." *Innova Hosp. San Antonio, Ltd. P'ship v. Blue Cross & Blue Shield of Ga., Inc.*, 892 F.3d 719, 730 (5th Cir. 2018) (cleaned up). Such allegations won't work here, however. There is no sign that Horne is in a better position to know whether Chizek's PII was stolen in the breach. *See* [28-1] at 2 ("[T]he investigation . . . was unable to confirm what information within [Horne's] systems was actually accessed."). And Chizek's allegations do not support a plausible inference that his PII was stolen during the breach.

He gives no timeline of how soon after the breach he started to experience fraudulent activity. And despite Chizek's care with his PII, "an individual's PII . . . can be stolen in myriad ways, often without the individual's knowledge." *Williams*, 737 F. Supp. 3d at 425. That Chizek does not share unencrypted PII on the internet does not lead to a plausible inference that his PII could only have been stolen in the breach. This is because Chizek fails to link the PII obtainable from the Horne data breach with his PII listed on the dark web. *See id.* at 424 (quoting *Blood v. Labette Cnty. Med. Ctr.*, No. 5:22-CV-4036, 2022 WL 11745549, at *8 (D. Kan. Oct. 20,

2022)). Lastly, he does not link the spam communications to the breach. Other courts have noted that "[s]pam calls, texts, and e-mails have become very common in this digitized world." *McCombs v. Delta Grp. Elecs., Inc.*, 676 F. Supp. 3d 1064, 1074 (D.N.M. 2023). Without more, Chizek "seems to simply be one among the many of us who are interrupted in our daily lives by unsolicited calls." *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 33 (D.D.C. 2014). This is not enough to infer that the Horne breach caused the spam communications.

In essence, Chizek asks the Court to conclude that someone stole his PII in the breach just because he later experienced fraud. But this would involve two logical errors. First, the Court would have to assume that the breach caused the fraud just because the fraud happened afterward. This is an example of a fallacy called *post hoc ergo propter hoc*. Second, the Court would have to assume that someone used Chizek's stolen PII from the breach to commit the fraud, but that assumption relies on the belief that someone stole his PII in the breach. This is circular reasoning. Neither rationale can support a reasonable inference that someone stole Chizek's data in the breach. *See Williams*, 737 F. Supp. 3d at 424–25; *see also Masterson v. IMA Fin. Grp., Inc.*, No. 2:23-CV-2223, 2023 WL 8647157, *4 (D. Kan. Dec. 14, 2023).[5]

[5] While the Court finds that Hemphill did not plausibly allege an injury in fact, even if she did, she would fail to allege causation, too. Hemphill has only one well-pleaded allegation that the breach harmed her: someone tried to access her bank account 18 months after the breach. [28] ¶ 121. This allegation is nearly identical to Chizek's and fails to establish causation for the same reasons.

Perhaps Chizek's PII was stolen in the breach and misused, but Chizek has "not nudged" those allegations "across the line from conceivable to plausible." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

B. Declaratory and Injunctive Claims

Hemphill and Chizek's claims for declaratory and injunctive relief also fail for lack of standing. [28] ¶¶ 217–25. Their claims turn on redressability, the third element of standing. Redressability requires it to be "likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Dobbin Plantersville Water Supply Corp. v. Lake*, 108 F.4th 320, 325 (5th Cir. 2024) (cleaned up). Declaratory or injunctive relief cannot remedy past harms. *Stringer v. Whitley*, 942 F.3d 715, 720 (5th Cir. 2019). So plaintiffs seeking prospective relief "must face a real and immediate threat of repeated injury." *Murthy*, 603 U.S. at 58 (cleaned up). In other words, the threatened injury must be either certainly impending or at substantial risk of occurring. *Id.*; *see also Attala Cnty. Branch of NAACP v. Evans*, 37 F.4th 1038, 1043 (5th Cir. 2022) ("We see no necessary difference between the concepts of a substantial risk and a real and immediate threat, though immediacy does imply a short timeframe."). Past injuries "are relevant only for their predictive value." *Murthy*, 603 U.S. at 59.

Moreover, redressability and causation "are often flip sides of the same coin" because remedying a future harm requires enjoining its cause. *All. for Hippocratic Med.*, 602 U.S. at 380 (cleaned up). For that reason, a court "cannot redress injury

that results from the independent action of some third party not before the court." *Murthy*, 603 U.S. at 57 (cleaned up).

Hemphill and Chizek seek a judgment declaring that Horne owes them a legal duty to secure their PII and continues to breach this duty. [28] ¶ 221. They also request an injunction requiring Horne to strengthen its data-security protocols, submit to annual data-security audits, and provide them with long-term credit monitoring. *Id.* ¶ 205. Even if Hemphill and Chizek's PII were exposed during the breach, enjoining Horne now would not redress any harms that Hemphill and Chizek may have already suffered. Likewise, an injunction would not remedy any injuries they might later suffer at the hands of independent third parties.

Thus, Hemphill and Chizek must show at least a substantial risk that Horne will soon lose their PII in another data breach. *Cf. Murthy*, 603 U.S. at 58. To that end, Hemphill and Chizek claim that "[t]he risk of another such breach is real, immediate, and substantial." [28] ¶ 223. In support of this conclusory assertion, they plead that Horne suffered one data breach, *id.* ¶ 43, and that PII is a valuable commodity prized by cybercriminals. *Id.* ¶ 58. So is one past data breach—combined with cybercriminals' unquenchable thirst for personal data—sufficiently predictive of another data breach in Horne's near future? No.

Mere "allegations of possible future injury do not suffice" to establish an imminent threat of future injury. *Attala Cnty.*, 37 F.4th at 1042 (cleaned up). While cybercriminals act in predictable ways, the mere existence of malevolent actors in cyberspace does not put Horne at constant risk of an imminent cyberattack. And

one data breach does not evidence a pattern of repeated cyberattacks on Horne that would permit the Court to predict that another data breach is certainly impending. Of course, another cyberattack on Horne is possible, but that possibility remains speculative.

C. Leave to Amend

In the final paragraph of their [22] Response, Hemphill and Chizek "request leave to amend" the [28] Second Amended Complaint if the Court grants Horne's [17] Motion to Dismiss. [22] at 26; *see also* Fed. R. Civ. P. 15(a). This request is procedurally improper, *see* L.U. Civ. R. 7(b)(3)(C), and "bare bones." *Porretto*, 113 F.4th at 491. A bare bones request "remains futile when it fails to apprise the district court of the facts that the plaintiff would plead in an amended complaint." *Id.* (cleaned up). And "although plaintiffs should ordinarily be offered an opportunity to amend if it appears that a more carefully drafted complaint might state claims upon which relief could be granted, that course need not be followed here since [Hemphill and Chizek] have already twice amended their complaint." *Herrmann Holdings Ltd. v. Lucent Techs. Inc.*, 302 F.3d 552, 566 (5th Cir. 2002) (cleaned up). Thus, the Court denies Hemphill and Chizek's barebones request to amend.

IV. Conclusion

For the reasons stated above, the Court GRANTS Horne's [17] Motion to Dismiss and DISMISSES Hemphill and Chizek's claims WITHOUT PREJUDICE for lack of standing. In doing so, the Court has considered all the parties'

arguments. Those arguments not addressed would not have altered the Court's decision. The Court will enter a separate final judgment consistent with this Order.

SO ORDERED, this 10th day of March, 2025.

s/ *Kristi H. Johnson*
UNITED STATES DISTRICT JUDGE